

# 3 Major Benefits of Cloud Migration: Cloud Compliance

Part of a secure cloud migration strategy is ensuring compliance of all the moving pieces. Just like your cloud journey, cloud compliance isn't all about the final destination. Discover how to leverage cloud security tools to ensure compliance is met along the way.

After the unforeseen acceleration of [cloud adoption due to the COVID-19](#) pandemic, many organizations hastily launched their services into the cloud to stay afloat. But these rapid transitions often come at the cost of neglecting compliance, which can result in not only hefty fines but [damage to reputation and customer trust](#). It's like a homebuilder hurrying to meet a deadline without double checking if everything is up to code and all the appropriate permits are filed. The deadline may be met—but if the roof collapses or a wall falls over, the consequences will be dire.

Governmental institutions have responded to the mass cloud adoption by [developing new data privacy and regulatory laws](#), and compliance organizations continue to create

more relevant [frameworks for cloud computing](#). As more organizations migrate to the cloud, compliance standards and rules will evolve in tandem. That's why it's critical to implement a scalable security strategy that can grow throughout your migration and keep up with cloud compliance requirements. Keep in mind that being compliant doesn't have to be a "do it or else" situation. Approaching cloud compliance as an enabler to operational excellence can motivate security and development teams to play their part and bridge the gap. [DevSecOps](#), anyone?

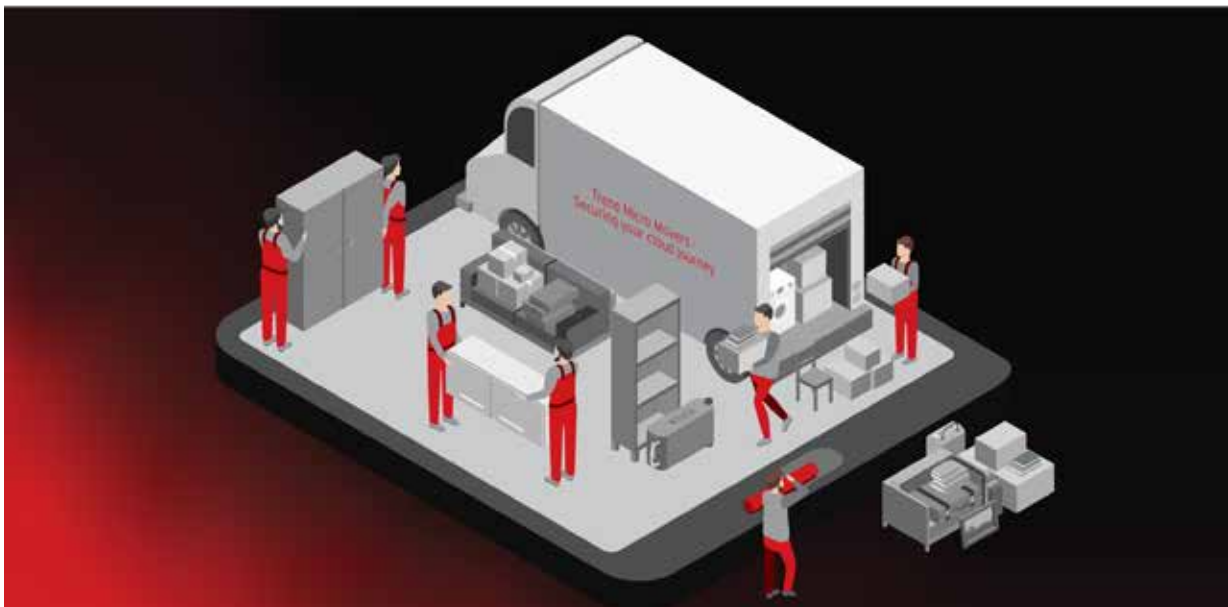
Let's take a look at the basics of cloud compliance and how to circumvent associated challenges.

## Compliance 101

[Compliance](#) seems like it's shrouded in mystery and requires a ton of labor-intensive work, but it's really quite simple. Basically, compliance is like a home inspection—it's all about ticking the right boxes and making sure everything works properly in order to prevent damage in the future.

In the case of cloud compliance, organizations must have the proper procedures in place to meet regulations applicable to their industry, such as GDPR, [PCI DSS](#), [HIPAA](#), [ISO](#), and more. There are also compliance standards and frameworks like the [NIST Cybersecurity Framework](#), CIS Benchmarks™, and [AWS Well-Architected Framework](#) that aren't mandatory but are great tools to help you stay on the good side of the other guys.

While compliance laws and standards may differ across industries and regions, they often address the same challenges:



**Data transfer:** Just as you're required to change your driver's license after a move, you must abide by the applicable national and regional privacy regulations when moving your data.

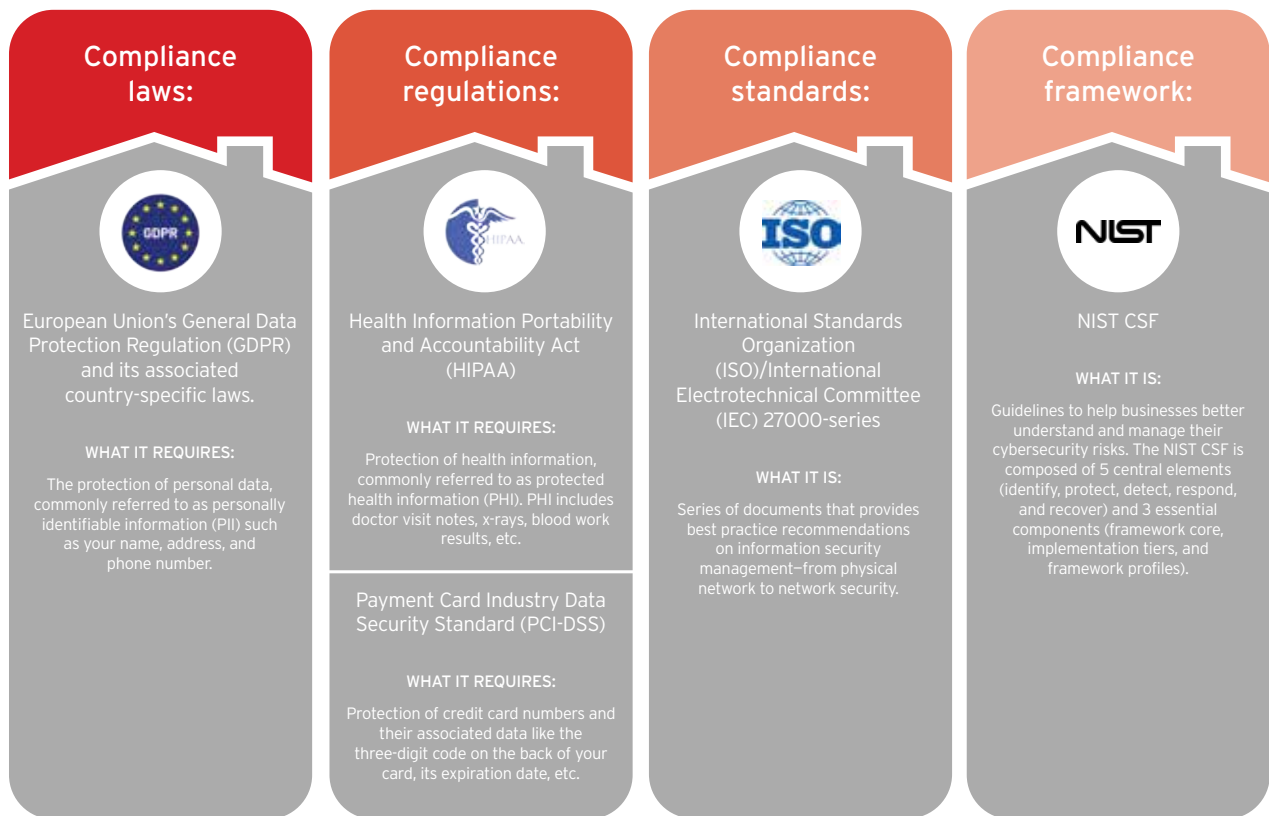
**Data visibility:** According to [Flexera](#), 82% of enterprises have a hybrid cloud strategy. While the hybrid cloud approach is popular, the distribution of storage can make securing it more complex. Make sure you have an eye on all your sensitive data—out of sight, out of mind is NOT the right approach here.

**Data security responsibility:** Ah, the [shared responsibility](#)

**model.** Your datacenter is just the host—you are responsible for securing it. Think of it like a safe in your home. If you keep it unlocked and you get robbed, you can't sue the safe manufacturer. It's 100% your responsibility to secure your data and therefore 100% your responsibility to be compliant in doing so.

**Data access:** You wouldn't give everyone you pass on the street a key to your home. The same applies in the cloud. Cloud compliance regulations are designed to help you limit access to a least-privilege level so you can avoid a breach.

We briefly mentioned a few of the well-known compliance standards—let's take a deeper look:



## How to achieve continuous compliance

So, where do you start? Your first step should be identifying which security tool will best meet the needs of ever-changing compliance standards and will keep up with your evolving infrastructure. As we discussed in [our last article](#), a security services platform is ideal. Here's how it can help you with the four compliance challenges we mentioned earlier:

### Challenge #1: Data transfer – Localized protection

Unlike point products, a platform can be deployed across multi- and hybrid-cloud environments so you can run continuous scans and audits to ensure compliance, wherever your data may be.

### Challenge #2: Data visibility – Enhanced insights

On-premises solutions only provide network-level insights, and

your cloud service provider (CSP) can't tell you the entire story due to privacy concerns. A platform enhances visibility across networks, security layers, and more so compliance issues can be identified and remediated quickly.

### Challenge #3: Data security responsibility – [Automated guardrails](#)

Say goodbye to the tedious task of manually monitoring, configuring, and maintaining your systems to stay compliant. Automated operational controls also ensure rules are enforced at scale—so you stay compliant as your business grows.

### Challenge #4: Data access – [Centralized identity and access management \(IAM\)](#)

One console for easy management of all your permissions, accounts, passwords, and policies. Think of it like a thermostat in your home—one place to control the temperature—versus radiators in each room that must be individually monitored and managed.

The next step is identifying which platform is best. There's no shortage of offerings available, but they're not all equal. To achieve your cloud compliance goals, look for specific features and functions, such as:

- **Intrusion detection and protection for each sever across every type of cloud environment, examining all incoming and outgoing traffic for protocol and policy violations or content that signals an attack.**
- **Virtual patching is like stopping a leak with heavy-duty plumbing repair tape while you wait for a plumber to come out and actually fix it. In this case, a virtual patch provides an extra layer of security against vulnerabilities while you wait for the official vendor patch. This helps you avoid any additional exploits that try to target the vulnerability.**
- **Integrity monitoring for critical operation system and application files (directories, registry keys, and values) to detect and report unexpected changes in real time.**
- **Malware prevention that leverages file reputation, behavioral analysis, machine-learning, and other advanced techniques to protect your systems.**
- **Localized/specific compliance measures across the broadest range of industry, geographic, and cybersecurity regulations and standards.**
- **Advanced threat intelligence as part of the platform for visibility into the entire threat landscape to protect against current and future threats.**

Remember, you are solely responsible for securing and maintaining compliance for your data. You wouldn't close your eyes and pick any home in a real estate flyer to purchase, so evaluate all your options carefully to make sure that your security and compliance needs will be met today, and in the future.

---

## Automated compliance with Trend Cloud One™ – Conformity

In the cloud computing world, conforming to compliance standards and regulations sets you up for success.

**Trend Cloud One™ – Conformity** can help you follow the rules to avoid breaches and fines while driving innovation and bridging the gap. Conformity is one of eight security solutions that compose the **Trend Cloud One™ platform**:

- **Trend Cloud One™ – Workload Security: Runtime protection for virtual, physical, cloud, and container workloads**
- **Trend Cloud One™ – Container Security: [Automated image scanning in your build pipeline](#)**
- **Trend Cloud One™ – File Storage Security: [Security for cloud file and object storage services](#)**
- **Trend Cloud One™ – Network Security: Cloud network layer intrusion protection system (IPS) security**
- **Trend Cloud One™ – Conformity: [Cloud security and compliance posture management](#)**
- **Trend Cloud One™ – Open Source Security by Snyk: Visibility and monitoring of open source vulnerabilities and license risks**
- **Trend Micro™ Cloud Sentry: Visibility of the threats in your AWS environment with quick, actionable insights in the context of your application**

Check out how Conformity can help tackle the four compliance challenges:

### Challenge #1: Data transfer

Monitor the compliance of all your cloud environments across different regions from one dashboard, so you can identify and remediate unwanted vulnerabilities and build to industry best practices.

### Challenge #2: Data visibility – Enhanced insights

Conformity provides real-time visibility of your entire infrastructure through a single, multi-cloud dashboard, giving you true situational awareness.

### Challenge #3: Data security responsibility – Automated guardrails

Auto-check against nearly 1,000 cloud service configurations across major CSPs, auto-remediate violations, and run scans against hundreds of industry best practice and compliance checks. Customize audit reports with endless combinations of filters and prioritized alerts so you can stay organized.

### Challenge #4: Data access – Centralized IAM

Ensure that your IAM policies are enforced with several automated IAM configuration checks. If any high-risk access violations are discovered, auto-remediation takes care of it.

Not only does Conformity address these common cloud compliance challenges, but you can also:

- **Remediate like a pro:** You and the DevOps teams don't have to be compliance experts to remediate threats. Every recommendation in Conformity is actionable—with clear step-by-step guides in our [Knowledge Base](#).
- **Enable a DevSecOps culture:** Infrastructure as code (IaC) means the most secure and compliant templates are deployed. Conformity also integrates seamlessly into your CI/CD pipeline with powerful APIs. Improve communication and collaboration between SecOps and DevOps teams by connecting it to your favorite third-party communication provider like Slack, Jira, Microsoft Teams, and more.
- **Monitor your progress:** Track the evolution of your compliance posture within the Conformity dashboard. Your compliance progress is measured against the AWS Well-Architected Framework and based on the daily compliance score average. Now you can focus in on which areas need more support.



Make sure your cloud is up to code throughout your cloud journey with automated compliance checks and remediation. Get started with a [free 30-day trial](#) of Conformity.

©2023 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo, OfficeScan and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [BLG01\_Cloud\_Migration\_Benefits\_Compliance\_230418US]

For details about what personal information we collect and why, please see our Privacy Notice on our website at: [trendmicro.com/privacy](https://trendmicro.com/privacy)